UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,698	12/27/2004	Marc Girault	P1907US	6941

8968 7590 05/21/2008

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

EXAMINER	
SU, SARAH	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,698	GIRAULT ET AL.	
	Examiner	Art Unit	
	Sarah Su	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☒ Claim(s) *1-6 and 12-18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/22/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Preliminary amendment, received on 27 December 2004, has been entered into record. In this amendment, claims 1-18 have been amended and claims 19-30 have been added.

Priority

2. The claim for priority from PCT/FR03/02000 filed on 27 June 2003 is duly noted.

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

4. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

5. The abstract of the disclosure is objected to because "module" on lines 4 and 8 should read –modulus–. Correction is required. See MPEP § 608.01(b).

6. The disclosure is objected to because of the following informalities:

   a. in page 28, line 27: "the index p" should read –the index j–;

   b. in page 31, line 3: "are designed" should read –is designed–;

c. in page 31, line 14: "communication means 34 are" should read –communication means 34 is–;

d. in page 31, line 24: "calculation means 37 are" should read –calculation means 37 is–.

Appropriate correction is required.

Claim Objections

7. Claims 1-6, 12-15, 16-18 are objected to because of the following informalities:

a. In claims 1-6, 12-14, 16, it is noted that the symbol "-" has been used but is non-functional. The Examiner requests that these be removed.

b. In claim 12, line 9: "second entity" is unclear if it relates to "a second entity" (claim 1, line 3);

c. In claim 12, line 10: "first exponent" is unclear if it relates to "a first exponent" (claim 1, line 4);

d. In claim 13, line 8: "to generate" should read –for generating–;

e. In claim 14, lines 3 and 7: "calculation means are" should read –calculation means is–;

f. In claim 15, line 2; claim 17, lines 2 and 3; claim 18, lines 2 and 3: "means are" should read –means is–.

Appropriate correction is required.

Drawings

8. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because:

a. reference character "13" has been used to designate both the step of transmitting y to B (Figure 1) and the step of transmitting y to C (Figure 5);

b. reference character "16" has been used to designate both the receiving of y at B (Figure 1) and the receiving of Y at B (Figure 5);

c. reference character "17" has been used to designate both calculating verification using y (Figure 1) and calculating verification using Y (Figure 5);

d. In Figure 4, element 28: "libre" should read –free–;

e. "step 23" has been used to designate both generating a first element of proof (page 25, lines 7-12) and generating the common number (page 25, lines 14-15);

f. they do not include the following reference sign(s) mentioned in the description: step 1 (page 25, line 7).

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are

not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1 and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. The terms "substantially less" in claim 1, line 13 and "substantially greater" in claim 8, lines 2-3 are relative terms which render the claims indefinite. The terms "substantially less" and "substantially greater" are not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. As a result, the language does not provide a clear definable value of resources consumed in claim 1 and the value of the private key in claim 8.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claim 13 is rejected under 35 U.S.C. 102(b) as being anticipated by Gilbert et al. (US Patent 5,987,138 and Gilbert hereinafter).

Gilbert discloses a system and method for identification and signature verification, the system and method having:

calculation means for generating a first element of proof (i.e. x) **completely or partly independently of the transaction and to generate a second element of proof** (i.e. y) **related to the first element of proof and dependent on a common number** (i.e. a_i) **specific to the transaction** (col. 7, lines 32-33, 43-45)**;**

communication means for transmitting at least the first and second elements of proof (i.e. x and y) **and for transmitting said common number** (i.e. set of numbers) **to the verifier device or receiving said common number from the verifier device** (col. 7, lines 32-33, 40-41, 51)**.**

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

16. Claims 1-2, 11, 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of M'Raihi et al. (US Patent 5,946,397 and M'Raihi hereinafter).
As to claims 1 and 16, Gilbert discloses:

> **generating a first element of proof** (i.e. x) **at the first entity** (i.e. claimant)**, whereby calculation of said first element of proof is executable independently of the transaction** (col. 7, lines 32-33)**;**
>
> **generating, at the first entity, a second element of proof** (i.e. answer y) **related to the first element of proof and dependent on a common number** (i.e. a_i) **shared by the first and second entities specifically for the transaction, whereby calculation of said first element of proof consumes substantially less resources than the calculation of said first element of proof** (col. 7, lines 43-45).

Gilbert does not disclose:

verifying, at the second entity that the first element of proof is related through a relationship with a first power modulo the modulus of a generic number having a second exponent equal to a linear combination of at least part of the common number and of the first exponent of the public key multiplied by the second element of proof.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert, as evidenced by M'Raihi.

M'Raihi discloses a system and method for cryptography with public key based on the discrete logarithm, the system and method having:

verifying, at the second entity that the first element of proof (i.e. x) **is related through a relationship with a first power modulo the modulus** (i.e. p) **of a generic number** (i.e. g) **having a second exponent** (i.e. k) **equal to a linear combination of at least part of the common number and of the first exponent of the public key multiplied by the second element of proof** (col. 2, lines 4-49).

Given the teaching of M'Raihi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert with the teachings of M'Raihi by verifying a relationship through the use of a linear combination exponent. M'Raihi recites motivation by disclosing that an exponent is necessary for each signature and creating an exponent using small coefficients in a linear combination would prevent attacks (col. 5, lines 49-52). It is obvious that the teachings of Gilbert would have benefited from the teachings of M'Raihi

by using an exponent in the form of a linear combination in order to create a signature that is protected against attacks.

As to claim 2, Gilbert discloses:

> **wherein for identifying the first entity, the first element of proof** (i.e. x) **is generated by the first entity by raising the generic number** (i.e. r) **to a second power modulo the modulus** (i.e. n) **having a third exponent equal to the first exponent of the public key** (i.e. e) **multiplied by a random integer kept secret by the first entity** (col. 7, lines 32-33)**;**
>
> **wherein the common number** (i.e. a_i) **is chosen randomly from within a security interval [0, t 1]** (i.e. 0, e-1) **and then sent by the second entity** (i.e. verifier) **after having received the first element of proof** (col. 7, lines 38-39)**;**
>
> **wherein the relationship verified by the second entity** (i.e. verifier) **is an equality relationship between a power of the first element of proof** (i.e. x) **and the first power of the generic number** (col. 7, lines 54, 62-63)**.**

As to claim 11, Gilbert discloses:

> **wherein the generic number is transmitted with the public key, the generic number being equal to a simple number raised to a power modulo the modulus with the private key as exponent** (col. 7, lines 19-22)**.**

As to claim 17, Gilbert discloses:

wherein the communication means are designed to receive the second element of proof (i.e. y) (col. 7, line 51) **and wherein the calculation means are designed to calculate the second exponent and said first power of the generic number** (col. 7, line 47).

17. Claims 12 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of M'Raihi as applied to claims 1 and 16 above, and further in view of Brickell (US Patent 7,165,181 B2).

As to claims 12 and 18, Gilbert in view of M'Raihi does not disclose:

receiving the second element of proof at a third entity;

generating a third element of proof at the third entity by raising the generic number to a power modulo the modulus with the second element of proof as exponent;

sending the third element of proof to the second entity;

at second entity, raising the third element of proof to a power of first exponent, modulo the modulus, and multiplying the result thereof by the generic number raised to a power whose exponent is the common number in order to verify the relationship relating the first element of proof to the second element of proof.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi, as evidenced by Brickell.

Brickell discloses a system and method for establishing trust without revealing identity, the system and method having:

receiving the second element of proof (i.e. m') **at a third entity** (i.e. Certifying Manufacturer) (col. 5, lines 1-2)**;**

generating a third element of proof (i.e. c') **at the third entity by raising the generic number to a power modulo the modulus with the second element of proof as exponent** (col. 5, lines 2-3)**;**

sending the third element of proof to the second entity (i.e. device) (col. 5, line 3)**;**

at second entity, raising the third element of proof to a power of first exponent, modulo the modulus, (col. 5, lines 3-4) **and multiplying the result thereof by the generic number raised to a power whose exponent is the common number in order to verify the relationship relating the first element of proof to the second element of proof** (col. 5, lines 5-6; col. 6, lines 18-25)**.**

Given the teaching of Brickell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi with the teachings of Brickell by using a third entity and signature in the verification process. Brickell recites motivation by disclosing that a cryptographic protocol that achieves anonymity and security requirements without the use of a conventional trusted third party is needed (col. 1, lines 49-52), which can be achieved through the use of a trusted platform module that proves the possession of a signature without revealing the signature (col. 5, lines 8-10). It is obvious that the

teachings of Gilbert in view of M'Raihi would have benefited from the teachings of Brickell by using a third entity in the verification process in order to maintain security anonymously.

18. Claims 19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of M'Raihi as applied to claim 2 above, and further in view of Kasahara et al. (US Patent 6,788,788 B1 and Kasahara hereinafter).

As to claims 19 and 27, Gilbert in view of M'Raihi does not disclose:

> **wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number, wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi, as evidenced by Kasahara.

Kasahara discloses a system and method for cryptographic communication with high security, the system and method having:

> **wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number** (col. 16, lines 40-41)**, wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof** (col. 6, line 52)**, and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number** (col. 8, line 36; col. 9, line 1)**.**

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above in respect to claims 12 and 18 as to why it is obvious to apply the teachings of Kasahara and the use of small coefficients in a linear combination for the verification process to the teachings of Gilbert in view of M'Raihi.

19. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of M'Raihi as applied to claim 1 above, and further in view of Arditti et al. (US Patent 6,125,445 and Arditti hereinafter).

As to claims 3 and 4, Gilbert combined with M'Raihi discloses:

> **wherein the common number is chosen at random from within a security interval [0,t 1]** (i.e. 0, e-1) **and then sent by the second entity** (i.e. verifier) **after having received the first element of proof** (col. 7, lines 38-40).

Gilbert in view of M'Raihi does not disclose:

> **wherein for authenticating that a message received by the second entity comes from the first entity, the first element of proof is generated by the first entity by applying a hash function to the message and to the generic number raised to a second power modulo the modulus having a third exponent equal to the first exponent of the public key multiplied by a random integer kept secret by the first entity;**
>
> **wherein the relationship verified by the second entity is an equality relationship between the first element of proof and a result of said hash function applied to the message and to the first power of the generic number.**

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi, as evidenced by Arditti.

Arditti discloses a system and method for public key identification using two hash functions, the system and method having:

> **wherein for authenticating that a message received by the second entity comes from the first entity, the first element of proof** (i.e. H(y)) **is generated by the first entity by applying a hash function to the message and to the generic number raised to a second power modulo the modulus having a third exponent equal to the first exponent of the public key multiplied by a random integer kept secret by the first entity** (col. 5, lines 16-18);
>
> **wherein the relationship verified by the second entity is an equality relationship between the first element of proof and a result of said hash function applied to the message and to the first power of the generic number** (col. 5, lines 29-31).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi with the teachings of Arditti by using a hash function in order to verify a signature of an entity. Arditti recites motivation by disclosing that security can be increased by being able to perform identity verification without having to reveal secrets (col. 1, lines 11-13), which can be achieved through disguising information (such as through the use of a hash function). It is obvious that the teachings of Arditti would have improved the teachings of Gilbert in view of M'Raihi by

providing for use of a hash function for verification in order to increase security by performing verification without revealing secrets that could be used maliciously.

20. Claims 5-10, 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of M'Raihi and Arditti as applied to claims 3 and 4 above, and further in view of Kasahara.

As to claims 5 and 6, Gilbert combined with M'Raihi and Arditti discloses:

> **wherein, in the verified relationship, the first element of proof** (i.e. x) **is considered with an exponent power equal to the first elementary common number** (i.e. a_i) (col. 7, line 59).

Gilbert combined with M'Raihi and Arditti does not disclose:

> **wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number;**
>
> **wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof.**

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi and Arditti, as evidenced by Kasahara.

Kasahara discloses:

> **wherein the common number comprises first and second elementary common numbers** (i.e. coefficients)**, wherein the second element of proof** (i.e. t_z) **is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number** (col. 16, lines 40-41)**;**
>
> **wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number** (i.e. γ)**, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the first exponent of the public key** (i.e. A) **multiplied by the second element of proof** (i.e. v) (col. 6, line 52)**.**

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi and Arditti with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above as to claims 12 and 18 why it is obvious to apply the teachings of Kasahara and the use of

small coefficients in a linear combination for the verification process to the teachings of Gilbert in view of M'Raihi.

As to claim 23, Gilbert in view of M'Raihi and Arditti does not disclose:

> **wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi and Arditti, as evidenced by Kasahara.

Kasahara discloses:

> **wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number** (col. 16, lines 40-41)**, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof** (col. 6, line 52)**, and**

wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power (col. 4, line 1).

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi and Arditti with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above in respect to claims 12 and 18 as to why it is obvious to apply the teachings of Kasahara and the use of small coefficients in a linear combination for the verification process to the teachings of Gilbert in view of M'Raihi.

As to claims 7 and 24, Gilbert in view of M'Raihi and further in view of Arditti, combined with Kasahara discloses:

wherein the second element of proof (i.e. y) **is calculated modulo an image of the modulus via a Carmichael function** (i.e. g) **or modulo a multiple of the order of the generic number modulo the modulus** (col. 4, lines 48-50; col. 5, lines 7-8, 16-17) in order to disguise the base used to calculated a signature. Arditti recites motivation by disclosing that without the knowledge of the base value, a defrauder cannot correctly reply to the verifier (col. 3, lines 63-64). It is obvious that the teachings of Gilbert in view of M'Raihi combined with Kasahara would have benefited from the teachings of Arditti by hiding the base value in order to prevent a correct reply from an unauthorized entity.

As to claim 8, Gilbert, combined with M'Raihi, Arditti and Kasahara, discloses:

wherein the random number is substantially greater than the value of the private key (i.e. s) (col. 3, lines 35-36).

As to claims 9 and 25, Gilbert in view of M'Raihi further in view of Arditti, combined with Kasahara discloses:

wherein the random integer (i.e. m) **is less than an image of the modulus via a Carmichael function** (i.e. k) **or less than a multiple of the order of the generic number modulo the modulus** (col. 4, lines 48-50; col. 7, lines 4-5) in order to allow a claimant to be verified without revealing a secret. Arditti recites motivation by disclosing that when an integer is close to a multiple of k (following the Carmichael Theorem), then a claimant can be simulated without knowledge of a secret, thus preventing a defrauder from stealing the secret (col. 7, lines 5-9). It is obvious that the teachings of Arditti would have improved the teachings of Gilbert in view of M'Raihi combined with Kasahara by using an integer smaller than an image in order to allow a claimant to be verified without transferring a secret.

As to claims 10 and 26, Gilbert in view of M'Raihi further in view of Arditti, combined with Kasahara discloses:

wherein the third exponent (i.e. T) **is calculated modulo an image of the modulus via a Carmichael function** (i.e. g) **or modulo a multiple of the order of the generic number modulo the modulus** (col. 5, lines 7-8) in order to allow a claimant to be verified without revealing a secret. Please refer to the motivation as recited above in respect to claims 9 and 25 as to why it is obvious to apply the teachings of Arditti to the teachings of Gilbert in view of M'Raihi and Kasahara.

21. Claims 20-22, 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of M'Raihi and Kasahara as applied to claims 19 and 27 above, and further in view of Arditti.

As to claims 20 and 28, Gilbert in view of M'Raihi and Kasahara does not disclose:

wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi and Kasahara, as evidenced by Arditti.

Arditti discloses:

wherein the second element of proof (i.e. y) **is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the**

order of the generic number modulo the modulus (col. 4, lines 48-50; col. 5, lines 7-8, 16-17).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi and Kasahara with the teachings of Arditti by disguising the base used to calculate a signature. Please refer to the motivation as recited above in respect to claims 7 and 24 as to why it is obvious to apply the teachings of Arditti to the teachings of Gilbert in view of M'Raihi and Kasahara.

As to claims 21 and 29, Gilbert in view of M'Raihi and Kasahara does not disclose:

wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi and Kasahara, as evidenced by Arditti.

Arditti discloses:

wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus (col. 4, lines 48-50; col. 7, lines 4-5).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying

the teachings of Gilbert in view of M'Raihi and Kasahara with the teachings of Arditti by using an integer smaller than an image in a verification process. Please refer to the motivation as recited above in respect to claims 9 and 25 as to why it is obvious to apply the teachings of Arditti to the teachings of Gilbert in view of M'Raihi and Kasahara.

As to claims 22 and 30, Gilbert in view of M'Raihi and Kasahara does not disclose:

> **wherein the third exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus**.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of M'Raihi and Kasahara, as evidenced by Arditti.

Arditti discloses:

> **wherein the third exponent** (i.e. T) **is calculated modulo an image of the modulus via a Carmichael function** (i.e. g) **or modulo a multiple of the order of the generic number modulo the modulus** (col. 5, lines 7-8).

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of M'Raihi and Kasahara with the teachings of Arditti by using an image in a verification process. Please refer to the motivation as recited above in respect to claims 9 and 25 as to why it is obvious to apply the teachings of Arditti to the teachings of Gilbert in view of M'Raihi and Kasahara.

22. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert as applied to claim 13 above, and further in view of Kasahara.

As to claim 14, Gilbert discloses:

> **wherein the calculation means are, on the one hand, designed to generate a first random number and to raise a generic number to a second power modulo the modulus having a third exponent equal to the first exponent of the public key** (i.e. e) **multiplied by the random integer** (col. 7, lines 32-33)**.**

Gilbert does not disclose:

> **wherein the calculation means are, on the other hand designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert, as evidenced by Kasahara.

Kasahara discloses:

> **wherein the calculation means are, on the other hand designed to generate the second element of proof by taking the difference between the**

random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number (col. 6, line 52; col. 16, lines 40-41)**.**

Given the teaching of Kasahara, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert with the teachings of Kasahara by using small coefficients to create an exponent from a linear combination to be used in the verification process. Please refer to the motivation as recited above in respect to claims 12 and 18 as to why it is obvious to apply the teachings of Kasahara and the use of small coefficients in a linear combination for the verification process to the teachings of Gilbert in view of M'Raihi.

23. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert in view of Kasahara as applied to claim 14 above, and further in view of Arditti.

As to claim 15, Gilbert in view of Kasahara does not disclose:

wherein the calculation means are designed to carry out operations modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Gilbert in view of Kasahara, as evidenced by Arditti.

Arditti discloses:

> **wherein the calculation means are designed to carry out operations modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus** (col. 4, lines 48-50)**.**

Given the teaching of Arditti, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Gilbert in view of Kasahara with the teachings of Arditti by providing for a way to disguise a value used to calculated a signature. Please refer to the motivation as recited above in respect to claims 7 and 24 as to why it is obvious to apply the teachings of Arditti to the teachings of Gilbert in view of M'Raihi and Kasahara.

Prior Art Made of Record

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. MacKenzie et al. (US 2003/0059041 A1) discloses a method and system for two-party generation of DSA signatures.

b. Guillou et al. (US Patent 7,080,254 B1) discloses a system and method for proving authenticity of an entity or integrity of a message.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131